

Tổ chức tài chính, ngân hàng, công ty chứng khoán là “miếng mồi ngon” của tội phạm mạng

09:12 31/03/2024

Công ty Công nghệ Veritas mới công bố số liệu rằng, cứ 11 giây trôi qua, thế giới lại ghi nhận một vụ tấn công mạng nhằm vào các tổ chức, doanh nghiệp lớn, đặc biệt là lĩnh vực tài chính.

Tổ chức tài chính, ngân hàng, công ty chứng khoán là những đối tượng đặc biệt dễ bị tội phạm mạng hay còn gọi là hacker "lưu tâm", để xâm nhập vào hệ thống, chiếm quyền kiểm soát, đòi tiền chuộc.



Tổ chức tài chính, ngân hàng, công ty chứng khoán là “miếng mồi ngon” của tội phạm mạng. Ảnh internet.

Hành vi phạm tội có thể nguy trọng hơn, ảnh hưởng tới an ninh tiền tệ. Riêng tại Mỹ - quốc gia ghi nhận nhiều vụ hack tài chính nhất thế giới - năm 2021 đã ghi nhận thiệt hại lên tới hơn 400 triệu USD do các vụ xâm nhập an ninh mạng.

Lý giải nguyên nhân tại sao các tổ chức tài chính, ngân hàng, công ty chứng khoán... đang là “miếng mồi ngon” của tội phạm mạng, ông Võ Đổ Thắng -

Giám đốc Trung tâm an ninh mạng Athena phân tích: Kể từ năm 2018 khi nhóm hacker sử dụng virus WannaCry tấn công máy tính của Việt Nam thì tấn công mạng vào các tổ chức tài chính ngày càng gia tăng.

“Tấn công vào các tổ chức kinh tế, ngân hàng, công ty chứng khoán, bệnh viện, sàn thương mại điện tử, đơn vị logistic... ngày càng tăng vì hacker thu được lợi ích kinh tế lớn, lên tới hàng triệu USD mỗi vụ.

Bởi, hoạt động kinh doanh của các tổ chức tài chính, ngân hàng, công ty chứng khoán....diễn ra chủ yếu trên nền tảng online, dữ liệu người dùng lớn, số lượng giao dịch cũng lớn, giá trị kinh tế lớn nên tội phạm mạng đang nhắm tới”, ông Võ Đỗ Thắng nói.

Theo ông Võ Đỗ Thắng thì Việt Nam là nền kinh tế mới đang phát triển mạnh mẽ, kinh tế số được đẩy mạnh, giao dịch trên Internet ngày càng tăng, trong khi quy định pháp lý còn nhiều lỗ hổng nên tội phạm luôn rình rập. Chẳng hạn như hacker quốc tế tấn công một tổ chức tại Việt Nam để tống tiền bằng bitcoin, loại tiền điện tử này lại chưa bị ràng buộc bởi quy định pháp luật Việt Nam nên lực lượng chức năng khó truy tìm hay xử lý triệt để.



Tổ chức tài chính, ngân hàng, công ty chứng khoán là “miếng mồi ngon” của tội phạm mạng. Ảnh internet.

"Quan trọng hơn, qua quá trình làm việc, khảo sát, Athena thấy rằng, nhận thức của lãnh đạo các công ty, tổ chức tài chính với an ninh mạng còn khá thờ ơ. Thế nên sau khi xây dựng hệ thống, lãnh đạo công ty thường không quan tâm đến đầu tư cho an ninh mạng, cho phương án dự phòng. Điều này dẫn đến nếu sự cố xảy ra, các công ty sẽ lúng túng trong khắc phục và “thiệt đơn, thiệt kép”, ông Võ Đỗ Thắng cho biết.

Đánh giá về mức độ đầu tư cho an toàn, an ninh mạng của các tổ chức tài chính, ngân hàng, công ty chứng khoán... tại Việt Nam hiện nay, ông Vũ Ngọc Sơn, Giám đốc công nghệ của NCS cho rằng: “Các tổ chức này dường như được đầu tư nhiều hơn cả về công nghệ, giải pháp an toàn thông tin... so với doanh nghiệp ngành nghề khác. Có thể nói là họ đầu tư không thiếu!”.

Ông Vũ Ngọc Sơn nhận định, sự đầu tư này không đồng nghĩa với việc sẽ chặn được triệt để các cuộc tấn công mạng. Bởi lẽ, tội phạm mạng quốc tế có công cụ, công nghệ thuộc diện chuyên nghiệp, hiện đại, có mục tiêu tấn công rõ ràng. Thế nên, một khi các tổ chức này đã là đích nhắm của hacker thì xác suất xảy ra tấn công là không nhỏ.

Ông Vũ Ngọc Sơn dẫn chứng: VnDirec là một ví dụ. “Không một hệ thống nào khẳng định đủ đảm bảo an toàn vì công nghệ luôn đổi mới. Các nhóm hacker sẽ rà quét lỗ hổng trên hệ thống, mục đích để tìm ra điểm yếu và xâm nhập. Hacker tấn công vào lỗ hổng mà các tổ chức này không biết như lỗ hổng zero - day, lỗ hổng trong cấu trúc, trong nhân sự, phần mềm...”



Tổ chức tài chính, ngân hàng, công ty chứng khoán là “miếng mồi ngon” của tội phạm mạng. Ảnh internet.

Rất khó để các công ty sử dụng hệ thống tìm được lỗ hổng, đa số chỉ nhà sản xuất mới tìm ra được đoạn mã có lỗ hổng, update lại và từ đó mới có phương án khắc phục. Chúng ta có hệ thống kết nối toàn cầu nên việc các tổ chức, nhóm hacker trên thế giới nhòm ngó, tấn công không phải là điều gì mới.

Nhưng phương thức thủ đoạn của hacker ngày càng tinh vi, chúng sử dụng công nghệ quốc tế rất cao nên cơ quan, tổ chức tại Việt Nam không có hệ thống phòng thủ mang tiêu chuẩn quốc tế rất khó để chống lại được”, ông Vũ Ngọc Sơn nhấn mạnh.

Làm thế nào để phòng ngừa hiệu quả nhất các vụ tội phạm tấn công mạng, theo ông Vũ Ngọc Sơn thì, để có thể tấn công được vào một hệ thống nào đó, hacker cần xâm nhập hệ thống, “nằm vùng” một thời gian dài, thậm chí vài tháng để xem dữ liệu nào là quan trọng, lỗ hổng ở đâu...

Do đó, khi đã bị tấn công, các tổ chức cũng mất nhiều thời gian mới tìm được dấu vết tấn công, phân tích nhật ký hệ thống, đánh giá mức độ nghiêm trọng từ đó mới tìm cách khắc phục được. Một khi bị tấn công mạng, tổ chức tài chính, ngân hàng, công ty chứng khoán... sẽ bị thiệt hại lớn về uy tín, tài sản và gây rủi ro đến cả khách hàng.

Về công tác ứng phó với tấn công mạng, Bộ Thông tin và Truyền thông đã đưa ra mô hình phòng thủ 4 lớp, phù hợp với doanh nghiệp và tổ chức có dữ liệu quan trọng. Còn theo các chuyên gia, để phòng chống tấn công mạng, giải pháp quan trọng nhất là phải có hệ thống dự phòng tiêu chuẩn và phản ứng nhanh với sự cố.



Tổ chức tài chính, ngân hàng, công ty chứng khoán là “miếng mồi ngon” của tội phạm mạng. Ảnh internet.

Khi hệ thống chính bị tấn công, hoạt động sẽ lập tức chuyển sang hệ thống dự phòng, thời gian phải tính theo từng phút. Hệ thống dự phòng này hoạt động theo thời gian thực với hệ thống chính, phải có tính độc lập với hệ thống chính về logic, về vật lý, địa lý, thường ở 2 địa điểm khác nhau, thậm chí cả ở địa

phương khác nhau để ngoài nguy cơ bị tấn công mạng thì còn phòng rủi ro trong trường hợp cháy nổ, thiên tai... vẫn có thể cung cấp dịch vụ được.

Bên cạnh đó, công tác giám sát an ninh mạng cần phải được chú trọng. Sau khi đã trang bị hệ thống, cần giám sát, rà soát định kỳ. Với các tổ chức quan trọng như tài chính, ngân hàng, công ty chứng khoán... cần rà soát 3 - 4 lần/năm. Đồng thời, cần diễn tập thường xuyên các phương án để vừa có thêm kinh nghiệm thực chiến, vừa xem hệ thống vận hành có đúng hay không, sự phối hợp giữa các bên ra sao?

Đối với người dùng, các chuyên gia an ninh mạng khuyến cáo người dân cần bảo vệ dữ liệu cá nhân, không tùy tiện đăng tải các thông tin cá nhân lên mạng và thường xuyên đổi mật khẩu với các ứng dụng đang dùng trên mạng Internet.

Theo thống kê của Công ty cổ phần Công nghệ an ninh mạng Việt Nam (NCS) công bố cuối năm 2023, năm ngoái ghi nhận 13.900 vụ tấn công mạng vào các tổ chức tại Việt Nam, trung bình mỗi tháng xảy ra 1.160 vụ, tăng 9,5% so với năm 2022. Đặc biệt, trong 3 tháng cuối năm 2023 số vụ tấn công mạng tăng mạnh, lên tới 1.614 vụ trong 1 tháng, gấp rưỡi so với trung bình.

VnDirect là công ty chứng khoán có thị phần môi giới cổ phiếu đứng thứ ba trên sàn HoSE với 7,01% (số liệu tính tới năm 2023), chỉ sau VPS và SSI. Tính đến cuối năm 2023, tổng tài sản của công ty đạt hơn 41.000 tỷ đồng, vốn chủ sở hữu trên 12.100 tỷ đồng. VnDirect quản lý hơn 83.000 tỷ đồng tài sản và các khoản phải trả về tài sản của khách hàng.

Cùng đợt với VnDirect, Tổng Công ty CP Bảo hiểm Bưu điện (PTI) và Công ty TNHH MTV quản lý quỹ đầu tư chứng khoán I.P.A (IPAAM).

Xuân Hải (t/h)